IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	Messaoud Benantar		
Assignee:	International Business Machines Corporation		
Title:	Method and System for Public-Key-Based Secure Authentication to be Distributed Legacy Applications		
Serial No.:	09/821,079	Filing Date:	March 29, 2001
Examiner:	Christopher J. Brown	Group Art Unit:	2134
Docket No.:	AUS920010064US1	Customer No.	65362

FILED ELECTRONICALLY

Austin, Texas
March 3, 2008

PRE-APPEAL BRIEF REQUEST FOR REVIEW AND STATEMENT OF REASONS

Sir:

Applicant requests review of the final Office Action dated November 1, 2007 in the above-identified application. No amendments are being filed with the request. This request is being filed with a Notice of Appeal. The following sets forth a succinct, concise, and focused set of arguments for which the review is being requested.

CLAIM STATUS

In the final Office Action, the Examiner withdrew the previous rejection, but a new ground of rejection was asserted for rejecting pending claims 1-7, 14-20 and 25-31. In particular, claims 1, 3-6, 14, 16-19, 25, and 27-30 were rejected as obvious over U.S. Patent No. 6,892,307 to Wood in view of U.S. Patent No. 5,892,828 to Perlman; claims 2, 15 and 26 were rejected as obvious over Wood and Perlman in view of U.S. Patent No. 6,460,141 to Olden; and claims 7, 20 and 31 were rejected as obvious over Wood and Perlman in view of U.S. Patent No. 6,754,829 to Butt. On March 1, 2008, Applicant filed a Response to Final Office Action to traverse the new ground of rejection, but no response has been received to date.

REMARKS

A. Claims 1, 3-6, 14, 16-19, 25 and 27-30 Are Not Obvious Over Wood and Perlman

In response to the Examiner's rejection of claims 1, 3-6, 14, 16-19, 25 and 27-30 as being obvious over Wood in view of Perlman, Applicant respectfully requests reconsideration and withdrawal of the rejection because the Examiner has not established a *prima facie* case of

obviousness. To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974); In re Wilson, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). Where a rejection is based on the assertion that all claim limitations are found in a number of prior art references, the fact finder must determine "[w]hat the prior art teaches, whether it teaches away from the claimed invention, and whether it motivates a combination of teachings from different references." In re Fulton, 391 F.3d 1195, 1199-1200 (Fed. Cir. 2004).

As a preliminary matter, a *prima facie* case of obviousness has not been established because, as noted above, none of the references, alone or in combination, discloses or suggests authenticating client accesses at a controlled resource (e.g., a legacy application) before granting client access to the controlled resource by using a separate host system to extract and decrypt authentication data from the client that is then forwarded to the controlled resource for authenticating the client, as variously recited in claims 1, 14 and 25. *See, e.g.*, claim 1 ("forwarding the authentication data to a controlled resource which authenticates the client based on the authentication data before allowing the client to access the controlled resource.") and Application, Abstract. In particular, the Examiner appears to combine and conflate the host-based claim requirements of "extracting encrypted authentication data from the attribute certificate…" and "decrypting the encrypted authentication data to regenerate the authentication data." According to the Examiner, both of these requirements are met by Wood's description of "decrypting" (Wood, col. 18, lines 54-55). *See*, Final Office Action, pp. 2-3. While Applicant agrees that Wood discloses decrypting the encrypted login credentials, Applicant respectfully submits that the cited "decrypting" disclosure fails to meet the two, distinct claim requirements of "extracting encrypted authentication data from the attribute certificate…" and "decrypting the encrypted authentication data to regenerate the authentication data." At best, Wood discloses decrypting the encrypted login credentials (which, according to the Examiner, corresponds to the claimed "attribute certificate" requirement), but does not separately disclose decrypting encrypted authentication data that has been extracted from the attribute certificate/login credential.

In addition to the foregoing, the Examiner has conceded that "Woods fails to teach forwarding the authentication data to a controlled resource." Final Office Action, p. 3. The disclosure from Perlman cited by the Examiner (Perlman, Application Server 236 at Server Node

202b, col. 6, lines 28-35) to meet the "forwarding" claim requirement is likewise deficient, insofar as the information (e.g., the decrypted "application secret") forwarded to Perlman's "server node 202b" is not provided by an authenticating host that is separate from the client/user, but is actually provided by the user/workstation 210 directly! Rather than routing the authentication operations through a host (as claimed), Perlman discloses the following sequence: (1) the user/workstation 210 attempts to access the application 236; (2) in response, the application 236 issues an authentication inquiry to the user/workstation 210; (3) the API 214 at the user/workstation 210 requests the proper application secret for the application 236 from the directory services 202a; (4) in response, the directory services 202a sends the encrypted application secret; and (5) the user/workstation 210 decrypts and forwards the property application secret to the application 236. Perlman, col. 6, lines 18-40. Thus, Perlman discloses that the user/workstation 210 is central involved in the various authentication processes, so that the user/workstation 210 – and not a separate host – is the entity that forwards the application secrets to the controlled applications 236.

The reason for this deficiency is readily understood once the purpose of Perlman is taken into account. Rather than being concerned with granting access to controlled resources on the Internet, such as legacy applications (as is the case the Applicant's invention), Perlman's invention is directed to verifying the presence of a user when authenticating the user to different applications by providing each user with a hashed password value that is stored at the user's workstation "so that it may be readily accessible for authenticating the user to other applications of the system." Perlman, Abstract. Thus, the user/workstation is obtaining and forwarding authentication data to the application, not the host which performed the separately-recited "receiving," "extracting," and "decrypting" steps.

As seen from the foregoing (and putting aside for the moment the propriety of combining the Perlman and Wood references), a *prima facie* case of obviousness has not been established because neither Perlman nor Wood disclose or suggest a host that forwards the authentication data to a controlled resource which authenticates the client based on the authentication data before allowing the client to access the controlled resource. Accordingly, claims 1, 14 and 25 are allowable. To the extent that dependent claims 3-6, 16-19 and 27-30 each respectively incorporate the requirements of independent claims 1, 14 and 25, these dependent claims are likewise allowable, even though there are additional differences recited in the dependent claims.

For example, claims 4, 17 and 28 each variously recited "authenticating the client for access to the controlled resource based on the authentication data." To meet this requirement of claims 4, 17 and 28, the Examiner cites Perlman col. 6, lines 32-33, which discloses that "this arrangement provides efficient authentication of a user to various application programs or systems in a distributed network without burdening the user or consuming considerable bandwidth…." While the cited passage refers generally to "efficient authentication," there is no reference to authenticating the client based on the "authentication data" that was extracted and encrypted as claimed. For at least the foregoing reasons, Applicant respectfully requests that the obviousness rejections of claims 1, 3-6, 14, 16-19, 25 and 27-30 over Perlman and Wood be withdrawn and that the claims be allowed.

B. Claims 2, 15 and 26 Are Not Obvious Over Wood, Perlman And Olden

In response to the rejection of claims 2, 15 and 26 as being obvious over Wood, Perlman and Olden, Applicant respectfully requests reconsideration and withdrawal of the rejection because, as explained above with reference to independent claims 1, 14 and 25, none of the references disclose or suggest authenticating client accesses at a controlled resource (e.g., a legacy application) before granting client access to the controlled resource by using a separate host system to extract *and* decrypt authentication data from the client that is then forwarded to the controlled resource for authenticating the client. Olden does not remedy this deficiency.

To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974); In re Wilson, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). Putting aside for the moment to propriety of combining these three references, a *prima facie* case of obviousness has not been established because none of the Wood, Perlman or Olden references disclose Applicant's host-based authentication scheme for decrypting and forwarding authentication data to a "controlled resource" which authenticates the client based on the authentication data before allowing the client to access the controlled resource. For at least the foregoing reasons, Applicant respectfully requests that the obviousness rejections of claims 2, 15 and 26 over Wood, Perlman and Olden be withdrawn and that the claims be allowed.

C. Claims 7, 20 and 31 Are Not Obvious Over Wood, Perlman And Butt

In response to the Examiner's rejection of claims 7, 20 and 31 as being obvious over Wood, Perlman and Butt, Applicant respectfully requests reconsideration and withdrawal of the

rejection because, as explained above with reference to independent claims 1, 14 and 25, none of the references disclose or suggest authenticating client accesses at a controlled resource (e.g., a legacy application) before granting client access to the controlled resource by using a separate host system to extract *and* decrypt authentication data from the client that is then forwarded to the controlled resource for authenticating the client.

To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974); In re Wilson, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). Putting aside for the moment the propriety of combining these three references, a *prima facie* case of obviousness has not been established because none of the Wood, Perlman or Butt references disclose Applicant's host-based authentication scheme for decrypting and forwarding authentication data to a "controlled resource" which authenticates the client based on the authentication data before allowing the client to access the controlled resource. For at least the foregoing reasons, Applicant respectfully requests that the obviousness rejections of claims 7, 20 and 31 over Wood, Perlman and Butt be withdrawn and that the claims be allowed.

CONCLUSION

For at least the foregoing reasons, Applicant submits that the rejection of the pending claims should be removed and these claims should be allowed. Nonetheless, should any issues remain that might be subject to resolution through a telephonic interview, the examiner is requested to telephone the undersigned at (512) 338-9100.

FILED ELECTRONICALLY
March 3, 2008

Respectfully submitted,

/Michael Rocco Cannatti/

Michael Rocco Cannatti
Attorney for Applicant
Reg. No. 34,791